

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-182770

(43)Date of publication of application : 26.06.2002

(51)Int.Cl.

G06F 1/00

G06F 12/14

H04L 9/32

(21)Application number : 2000-384209

(71)Applicant : MATSUSHITA ELECTRIC IND CO  
LTD

(22)Date of filing : 18.12.2000

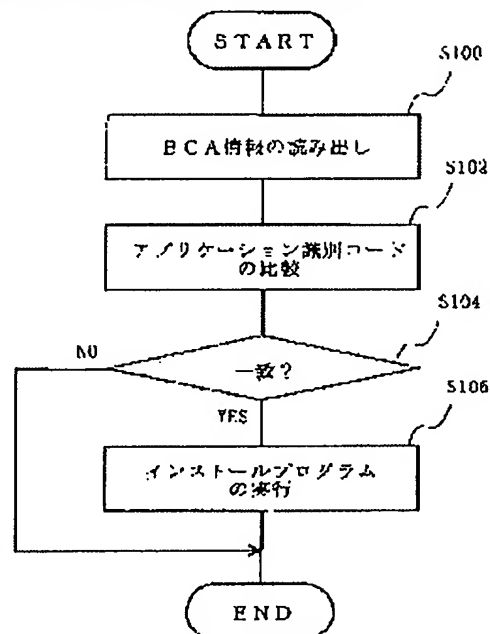
(72)Inventor : MORIYAMA YUKICHI  
NISHII KIYOSHI

## (54) RECORDING MEDIUM HAVING NORMAL USER AUTHENTICATION FUNCTION

## (57)Abstract:

PROBLEM TO BE SOLVED: To provide a recording medium capable of simplifying the authentication work of normal user and also preventing an illegal use by an illegal copy.

SOLUTION: First, identification information in a BCA area is read according to a normal user authentication program (S100). An application identification code included in the read identification information is compared with a normal application identification code described in the authentication program (S102), and whether or not the codes coincide with each other is judged (S103). When the codes coincide, the user of the read identification information is judged to be a normal user allowed to use the original disk, a software program is installed according to an install program (S104) and the processing is finished. Meanwhile, when the codes do not coincide, the user is judged to be an illegal user, the processing is finished without conducting the install program.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-182770  
(P2002-182770A)

(43) 公開日 平成14年6月26日 (2002. 6. 26)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコード <sup>*</sup> (参考)
G 0 6 F 1/00		G 0 6 F 12/14	3 2 0 A 5 B 0 1 7
	12/14	9/06	6 6 0 E 5 B 0 7 6
H 0 4 L 9/32	3 2 0	H 0 4 L 9/00	6 7 3 A 5 J 1 0 4

審査請求 未請求 請求項の数 6 O L (全 7 頁)

(21) 出願番号 特願2000-384209 (P2000-384209)

(22) 出願日 平成12年12月18日 (2000. 12. 18)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 森山 諭吉

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72) 発明者 西井 清

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(74) 代理人 100098291

弁理士 小笠原 史朗

Fターム (参考) 5B017 AA07 BA07 CA15

5B076 FA20 FB05

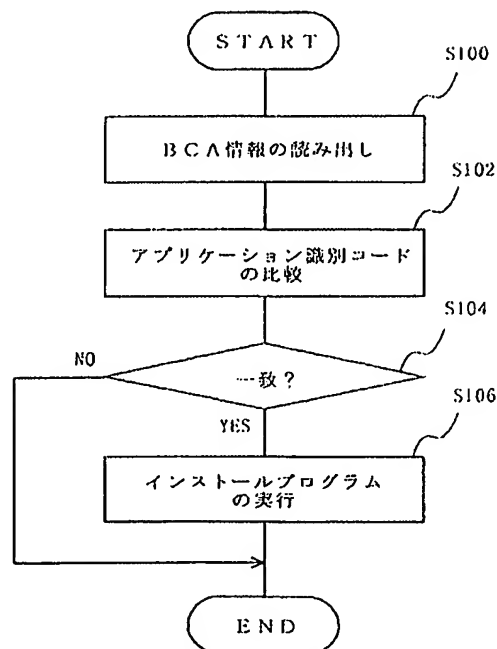
5J104 AA07 KA01 NA05 NA32 PA14

(54) 【発明の名称】 正規ユーザ認証機能付き記録媒体

(57) 【要約】

【課題】 ソフトウェアプログラムの不正コピーを防止するために手作業によりCDキーの入力を行うのは手間であり、不正防止に対する有効性にも欠ける。

【解決手段】 正規ユーザ認証プログラムに従って、まずBCA領域の識別情報を読み出す (S100)。そして、読み出した識別情報に含まれるアプリケーション識別コードと認証プログラムに記述されている正規のアプリケーション識別コードとを比較し (S102)、それらコードが一致するか否かを判定する (S103)。一致する場合にはオリジナルのディスクを使用する正規のユーザであると判断してインストールプログラムに従ってソフトウェアプログラムのインストールを実行し (S104)、処理を終了する。一方、一致しない場合には、不正なユーザであると判断してインストールプログラムを実行することなく処理を終了する。



## 【特許請求の範囲】

【請求項1】 コンテンツ読み出し端末にコンテンツを供給するためのコンピュータ読み取り可能な記録媒体であって、  
前記コンテンツ及び所定のプログラムを格納するデータ格納領域と、  
所定の固有情報を格納する書き換え不可能な領域とを備え、  
前記所定のプログラムは、  
前記コンテンツ読み出し端末に、  
前記所定の固有情報を読み出すステップと、  
当該読み出した所定の固有情報に基づいて正規ユーザの認証を行う認証ステップと、  
前記認証ステップの認証結果に応じて前記コンテンツを有効化する有効化ステップとを実行させるためのプログラムであることを特徴とする、正規ユーザ認証機能付き記録媒体。

【請求項2】 前記書き換え不可領域がDVDのBCA領域(Burst Cutting Area)であることを特徴とする、請求項1記載の正規ユーザ認証機能付き記録媒体。

【請求項3】 前記コンテンツがソフトウェアプログラムであり、  
前記有効化ステップは前記認証ステップの認証結果に応じて当該ソフトウェアプログラムをインストールすることを特徴とする、請求項1記載の正規ユーザ認証機能付き記録媒体。

【請求項4】 前記コンテンツが前記データ格納領域に暗号化して格納されており、  
前記有効化ステップは前記認証ステップの認証結果に応じて当該暗号化されたコンテンツを復号化することを特徴とする、請求項1記載の正規ユーザ認証機能付き記録媒体。

【請求項5】 前記所定の固有情報は前記コンテンツを識別するためのコンテンツ識別コードを含み、  
前記認証ステップは前記コンテンツ識別コードが正規のコンテンツ識別コードに一致するか否かを判断することによって正規ユーザの認証を行うことを特徴とする、請求項1記載の正規ユーザ認証機能付き記録媒体。

【請求項6】 前記所定の固有情報はチェックデジットを含み、  
前記認証ステップは前記固有情報に基づいて所定の演算を実行した結果が前記チェックデジットに一致するか否かを判断することによって正規ユーザの認証を行うことを特徴とする、請求項1記載の正規ユーザ認証機能付き記録媒体。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、正規ユーザ認証機能付き記録媒体に関し、より特定的には、コンテンツ読

み出し端末にコンテンツを供給するためのコンピュータ読み取り可能な記録媒体に関する。

## 【0002】

【従来の技術】従来、CD-ROMに記録されたソフトウェアをインストールして利用する場合、通常、インストール時やインストール後の起動時にCDキーの入力が必要となる。このとき、所定のCDキーの入力がなければ、ソフトウェアを利用することができない。

【0003】CDキーは、通常、CD-ROMやケースやマニュアルなどに記載されている。したがって、ソフトウェアを記録したCD-ROMを不正コピーした場合、不正コピーしたメディアを入手したユーザにはCDキーが分からない。このため、オリジナルのCD-ROMを購入した正規のユーザのみがソフトウェアを利用することができる。

## 【0004】

【課題が解決しようとする課題】しかしながら、上述の方法では、インストールする際などにユーザがCDキーを手作業で入力する手間を要し、また、CDキーを記載したケースやマニュアルについても紛失しないように管理しておく手間を要するという問題がある。

【0005】さらに、不正コピーしたメディアを入手したユーザがCDキーも同時に入手した場合、このユーザによるソフトウェアの不正利用を防止することができないという問題もある。

【0006】それ故に、本発明の目的は、正規ユーザの認証作業を簡略化でき、かつ不正コピーによる不正利用を防止することのできる記録媒体を提供することである。

## 【0007】

【課題を解決するための手段および発明の効果】第1の発明は、コンテンツ読み出し端末にコンテンツを供給するためのコンピュータ読み取り可能な記録媒体であって、前記コンテンツ及び所定のプログラムを格納するデータ格納領域と、所定の固有情報を格納する書き換え不可能な領域とを備え、前記所定のプログラムは、前記コンテンツ読み出し端末に、前記所定の固有情報を読み出すステップと、当該読み出した所定の固有情報に基づいて正規ユーザの認証を行う認証ステップと、前記認証ステップの認証結果に応じて前記コンテンツを有効化する有効化ステップとを実行させるためのプログラムであることを特徴とする。

【0008】上記のように、第1の発明によれば、書き換え不可能な領域に記録される固有の情報を用いてコンテンツの利用が制限されるため、ユーザがID等を手作業で入力することなしに認証を行い、オリジナルのメディア以外のメディアに不正コピーされたコンテンツの利用を防止することができる。

【0009】第2の発明は、第1の発明において、前記書き換え不可領域がDVDのBCA領域(Burst

Cutting Area)であることを特徴とする。

【0010】上記のように、第2の発明によれば、書き換え不可領域として、DVDに固有のBCA領域を利用することができる。

【0011】第3の発明は、第1の発明において、前記コンテンツがソフトウェアプログラムであり、前記有効化ステップは前記認証ステップの認証結果に応じて当該ソフトウェアプログラムをインストールすることを特徴とする。

【0012】上記のように、第3の発明によれば、認証結果に応じてソフトウェアプログラムのインストールを制限するため、不正コピーによるソフトウェアの不正利用を防止することができる。

【0013】第4の発明は、第1の発明において、前記コンテンツが前記データ格納領域に暗号化して格納されており、前記有効化ステップは前記認証ステップの認証結果に応じて当該暗号化されたコンテンツを復号化することを特徴とする。

【0014】上記のように、第4の発明によれば、認証結果に基づいて暗号化済みコンテンツの復号化を制限するため、不正コピーによるソフトウェアの不正利用を防止することができる。

【0015】第5の発明は、第1の発明において、前記所定の固有情報は前記コンテンツを識別するためのコンテンツ識別コードを含み、前記認証ステップは前記コンテンツ識別コードが正規のコンテンツ識別コードに一致するか否かを判断することによって正規ユーザの認証を行うことを特徴とする。

【0016】上記のように、第5の発明によれば、コンテンツ識別情報が正規のコンテンツ識別情報と一致するか否かを判断することによって、認証を容易に行うことができる。

【0017】第6の発明は、第1の発明において、前記所定の固有情報はチェックデジットを含み、前記認証ステップは前記固有情報に基づいて所定の演算を実行した結果が前記チェックデジットに一致するか否かを判断することによって正規ユーザの認証を行うことを特徴とする。

【0018】上記のように、第6の発明によれば、固有情報に基づく演算結果がチェックデジットに一致するか否かを判断することによって、不正利用をより効果的に防止することができる。

【0019】

【発明の実施の形態】以下、本発明の種々の実施形態について図面を参照して説明する。

(第1の実施形態) 図1は、本発明の第1の実施形態に係るDVD-ROMに記録されているソフトウェアプログラムをインストールする際のシステム構成を示すブロック図である。DVD-ROM100は、DVDドライブ300を介してユーザ端末200に接続される。ユー

ザ端末200のCPU210は、DVD-ROM100に記録されているプログラムに従って、ハードディスク220にソフトウェアプログラムをインストールする。

【0020】DVD-ROM100は、通常のデータ格納領域の他にBCA領域(Burst Cutting Area)10を有する。BCA領域10は、製造段階においてディスクの識別情報11が書き込まれる書き換え不可能な領域である。この識別情報11によってディスク毎の識別が可能となる。

【0021】通常のデータ格納領域には、正規ユーザ認証プログラム101、インストールプログラム102及びソフトウェアプログラム103が格納されている。認証プログラム101及びインストールプログラム102は、ソフトウェアプログラム103をハードディスク220にインストールする際にCPU210により実行されるプログラムである。認証プログラム101は、このメディア100が不正コピーされたものではないオリジナルのメディアであるか否かを判別して正規ユーザの認証を行うプログラムである。インストールプログラム102は、ソフトウェアプログラム103をインストールするためのプログラムである。

【0022】次に、図2を参照して、BCA領域10に格納される識別情報11について説明する。本実施形態では、一例として、BCA領域10にはディスクのプレス時に170バイトのアプリケーション識別コードと18バイトのシリアル番号を格納する。アプリケーション識別コードは同一のソフトウェアプログラムに対して共通に与えられる識別コードである。シリアル番号は共通のアプリケーション識別コードを有するグループに対してシリアルに与えられる識別番号である。

【0023】以下、図3のフローチャートを参照して、ソフトウェアプログラム103のインストール時のCPU210の動作について説明する。CPU210は、正規ユーザ認証プログラム101に従って、まずBCA領域10の識別情報11を読み出す(S100)。そして、読み出した識別情報11に含まれるアプリケーション識別コードと認証プログラム101に記述されている正規のアプリケーション識別コードとを比較し(S102)、それらコードが一致するか否かを判定する(S103)。一致する場合にはオリジナルのディスクを使用する正規のユーザであると判断してインストールプログラム102に従ってソフトウェアプログラム103のインストールを実行し(S104)、処理を終了する。一方、一致しない場合には、不正なユーザであると判断してインストールプログラム102を実行することなく処理を終了する。

【0024】次に、以上の動作によって不正コピーによるソフトウェアプログラムの不正利用が防止できることについて説明する。上述したように、DVD-ROMのBCA領域の情報は、ディスク製造時に記録され、以

後、書き換えることは不可能である。本実施形態に係るDVD-ROM100には、ディスク製造時に、BCA領域40に所定のアプリケーション識別コードを記録するとともに、正規ユーザ認証プログラム101に、このアプリケーション識別コードと同一の正規のアプリケーション識別コードを記述する。したがって、オリジナルのDVD-ROM100のインストール時には、これらアプリケーション識別コードが一致するため、正常にインストールを実行することができる。

【0025】一方、このDVD-ROM100の記録内容が他のメディアに不正コピーされた場合について説明する。例えば、コピー先のメディアがDVD-RAMである場合には、このDVD-RAMに正規ユーザ認証プログラム101、インストールプログラム102及びソフトウェアプログラム103がコピーされる。しかし、BCA領域に格納されている識別情報については書き換え不可能なためコピーされず、コピー先のDVD-RAMのBCA領域にはディスク製造時に記録された識別情報が記録されたままである。したがって、認証プログラム101に記述されている正規のアプリケーション識別コードと、BCA領域に格納されている識別情報が一致しないため、インストールは失敗に終わる。また、例えば、コピー先のメディアがCD-Rである場合には、BCA領域そのものがないので、インストールは失敗に終わる。

【0026】なお、本実施形態では正規ユーザの認証にアプリケーション識別コードを用いたが、これに限らず、例えばBCA領域内の識別情報全体をキー情報として用いることも可能である。ただし、その場合、ディスク毎にキー情報が異なってしまうため、認証プログラム101に記述しておく正規の識別情報も、ディスク毎に変える必要があり、製造時に手間がかかってしまう。したがって、本実施形態のように、シリアル番号を除いた共通の識別コードを認証のためのキー情報として用いるのが製造時の手間を省くという点では好ましい。

【0027】また、本実施形態では正規ユーザ認証プログラム101とインストールプログラム102をそれぞれ独立したプログラムとして説明したが、これに限らず、インストールプログラム102が認証プログラム101の機能を含んでも構わない。

【0028】また、本実施形態では認証時に用いる正規のアプリケーション識別コードは認証プログラム101に記述されているとしたが、これに限らず、DVD-ROM100内の他の領域に格納されていても構わない。

【0029】また、本実施形態ではDVD-ROM100に記録されるソフトウェアプログラム103は1つであるが、複数のソフトウェアプログラムを記録しても構わない。

【0030】以上のように、第1の実施形態によれば、インストール時等にCDキー等を手作業で入力すること

なしに正規ユーザの認証を行うことができるためインストール作業が簡略化され、さらに、認証のためのキー情報として、書き換え不可能なBCA領域内の情報を利用しているため、不正コピーによるソフトウェアプログラムの不正利用を防止することができる。

【0031】(第2の実施形態)図4は、本発明の第2の実施形態に係るDVD-ROMに記録されているソフトウェアプログラムをインストールする際のシステム構成を示すブロック図である。図4において、図1と同一の構成には同一の参照符号を付す。

【0032】第2の実施形態が第1の実施形態と異なる点は、BCA領域40内の識別情報41と、通常のデータ格納領域内の正規ユーザ認証プログラム401のみであるので、以下、これら相違点のみを説明する。

【0033】次に、図5を参照して、BCA領域40に格納される識別情報41について説明する。本実施形態では、一例として、BCA領域40にはディスクのプレス時に168バイトのアプリケーション識別コードと18バイトのシリアル番号と2バイトのチェックデジットとを格納する。チェックデジットは、正規ユーザの認証を行う際に用いられる情報である。

【0034】以下、図6のフローチャートを参照して、ソフトウェアプログラム103のインストール時のCPU210の動作について説明する。CPU210は、正規ユーザ認証プログラム401に従って、まずBCA領域40の識別情報41を読み出す(S200)。そして、読み出した識別情報41に含まれるアプリケーション識別コード及びシリアル番号の合わせて186バイトの情報に基づいて、認証プログラム401に記述されている演算を実行する(S202)。演算結果をチェックデジットと比較し(S204)、それらが一致するか否かを判定する(S206)。一致する場合にはオリジナルのディスクを使用する正規のユーザであると判断して、インストールプログラム102に従ってソフトウェアプログラム103のインストールを実行し(S208)、処理を終了する。一方、一致しない場合には、不正なユーザであると判断してインストールプログラム102を実行することなく処理を終了する。

【0035】次に、以上の動作によってソフトウェアプログラムの不正コピーによる不正利用が防止できることについて説明する。上述したように、DVD-ROMのBCA領域の情報は、ディスク製造時に記録され、以後、書き換えることは不可能である。本実施形態に係るDVD-ROM400には、ディスク製造時に、BCA領域40に所定のアプリケーション識別コード及びシリアル番号を記録するとともに、これらの情報に基づいて所定の演算を行った結果をチェックデジットとして記録し、正規ユーザ認証プログラム401に、この所定の演算方法を記述する。したがって、オリジナルのDVD-ROM400のインストール時には、BCA情報に基づ

く演算結果とチェックデジットが一致するため、インストールを実行することができる。

【0036】一方、このDVD-ROM400の記録内容が他のメディアに不正コピーされた場合については、コピー先のメディアに正規ユーザ認証プログラム401、インストールプログラム102及びソフトウェアプログラム103がコピーされる。しかし、BCA領域に格納されている識別情報については、書き換え不可能なためコピーされない。したがって、コピー先のメディアのBCA領域に格納されている識別情報に基づいて行われる認証プログラム401に記述されている演算の結果は識別情報内のチェックデジットと一致しないため、インストールは失敗に終わる。またコピー先のメディアにBCA領域がない場合にもインストールは失敗に終わる。

【0037】なお、本実施形態ではアプリケーション識別コード及びシリアル番号に基づいて演算を行ったが、これに限らず、例えばアプリケーション識別コード及びシリアル番号の一部を利用するとしても構わない。

【0038】また、本実施形態では、第1の実施形態と同様に、インストールプログラム102が認証プログラム101の機能を含んでも構わない。また、演算方法に関する情報は認証プログラム401に記述されているとしたが、DVD-ROM400内の他の領域に格納されていても構わない。

【0039】また、本実施形態ではDVD-ROM400に記録されるソフトウェアプログラム103は1つであるが、複数のソフトウェアプログラムを記録しても構わない。

【0040】以上のように、第2の実施形態によれば、インストール時等にCDキー等を手作業で入力することなしに正規ユーザの認証を行うことができるためインストール作業が簡略化され、さらに、認証のためのキー情報として、書き換え不可能なBCA領域内の情報を利用しているため、不正コピーによるソフトウェアプログラムの不正利用を防止することができる。そしてさらに、BCA領域内の識別情報に基づいて演算を行ってから認証を行うので、不正をより確実に防止することができる。

【0041】(第3の実施形態)図7は、本発明の第3の実施形態に係るDVD-ROMに記録されている映像コンテンツを再生する際のシステム構成を示すブロック図である。DVD-ROM500は、DVDドライブ300を介してユーザ端末600に接続される。ユーザ端末600のCPU610は、DVD-ROM500に記録されている暗号化済み映像コンテンツ503を読み出して表示装置630に表示する。

【0042】DVD-ROM500の通常のデータ格納領域には、正規ユーザ認証プログラム501、暗号解除プログラム504及び暗号化済み映像コンテンツ505が格納されている。認証プログラム501及び暗号解除

プログラム504は、暗号化済み映像コンテンツ505を再生する際にCPU610により実行されるプログラムである。

【0043】なお、BCA領域50に格納される識別情報51及び正規ユーザ認証プログラム501を用いたユーザ認証動作については第1の実施形態と同様とし、ここでは詳細な説明を省略する。

【0044】以下、図8のフローチャートを参照して、暗号化済み映像コンテンツの再生時のCPU610の動作について説明する。CPU610は、正規ユーザ認証プログラム501に従って、まずBCA領域50の識別情報51を読み出す(S300)。そして、読み出した識別情報51に含まれるアプリケーション識別コードと認証プログラム501に記述されている正規のアプリケーション識別コードとを比較し(S302)、それらコードが一致するか否かを判定する(S304)。一致する場合にはオリジナルのディスクを使用する正規のユーザであると判断して暗号解除プログラム504に従って暗号化済み映像コンテンツ505を復号化して映像コンテンツを再生し(S306)、処理を終了する。一方、一致しない場合には、不正なユーザであると判断して暗号解除プログラム504を実行することなく処理を終了する。

【0045】次に、以上の動作によって不正コピーによる映像コンテンツの不正利用が防止できることについて説明する。映像コンテンツは、ファイル単位で著作権保護が必要である。したがって、映像ファイルを不正コピーして利用することができないようにするためには、映像ファイルを暗号化しておく必要がある。暗号化した映像ファイルは、復号化しなければ利用することができない。そこで、本実施形態では、認証プログラム501によって、このメディアが不正コピーしたものではないオリジナルのメディアであると判断された場合のみ、この暗号化済み映像コンテンツ505を復号するための暗号解除プログラム504を有効化する。したがって、不正コピーされたメディアを再生することは不可能となる。

【0046】なお、本実施形態では正規ユーザの認証にアプリケーション識別コードを用いたが、これに限らず、例えばBCA領域内の識別情報全体をキー情報として用いることも可能である。また、チェックデジットを用いた認証を行うことも可能である。

【0047】また、本実施形態では正規ユーザ認証プログラム501と暗号解除プログラム504をそれぞれ独立したプログラムとして説明したが、これに限らず、暗号解除プログラム504が認証プログラム501の機能を含んでも構わない。

【0048】また、本実施形態ではDVD-ROM500に記録される暗号化済み映像コンテンツ505は1つであったが、複数の映像コンテンツファイルをそれぞれ暗号化して記録しても構わない。

【0049】以上のように、第3の実施形態によれば、映像コンテンツの再生時に、再生を行おうとする映像コンテンツの暗号化方式に対応した専用のデコーダ等を別途設けることなく暗号化済み映像コンテンツを再生することができるとともに、CDキー等を手作業で入力することなしに正規ユーザの認証を行うことができるため認証作業が簡略化され、さらに、認証のためのキー情報として、書き換え不可能なBCA領域内の情報を利用しているため、不正コピーによる映像コンテンツの不正利用を防止することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係るDVD-ROMを用いてソフトウェアプログラムをインストールする際のシステムの構成を示す図である。

【図2】第1の実施形態に係るDVD-ROMのBCA領域内の識別情報の構成の一例を示す図である。

【図3】第1の実施形態に係るDVD-ROMに記録されたソフトウェアプログラムのインストール時の動作を示すフローチャートである。

【図4】本発明の第2の実施形態に係るDVD-ROMを用いてインストールする際のシステムの構成を示す図である。

【図5】第2の実施形態に係るDVD-ROMのBCA領域内の識別情報の構成の他の一例を示す図である。

【図6】第2の実施形態に係るDVD-ROMに記録されたソフトウェアプログラムのインストール時の動作を示すフローチャートである。

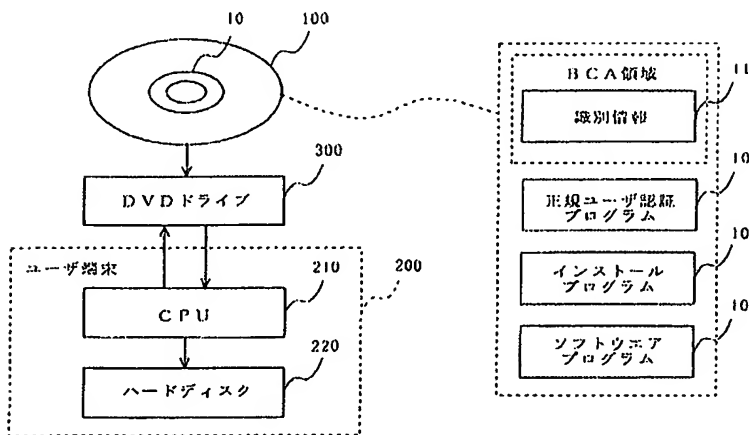
【図7】本発明の第3の実施形態に係るDVD-ROMを用いて映像コンテンツを再生する際のシステムの構成を示す図である。

【図8】第3の実施形態に係るDVD-ROMに記録された暗号化済み映像コンテンツの再生時の動作を示すフローチャートである。

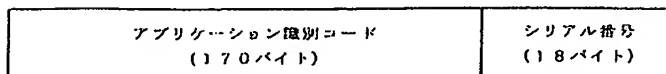
【符号の説明】

- 10 BCA領域
- 11 識別情報
- 40 BCA領域
- 41 識別情報
- 50 BCA領域
- 51 識別情報
- 100 DVD-ROM
- 101 正規ユーザ認証プログラム
- 102 インストールプログラム
- 103 ソフトウェアプログラム
- 200 ユーザ端末
- 210 CPU
- 220 ハードディスク
- 300 DVDドライブ
- 400 DVD-ROM
- 401 正規ユーザ認証プログラム
- 500 DVD-ROM
- 501 正規ユーザ認証プログラム
- 504 暗号解除プログラム
- 505 暗号化済み映像コンテンツ

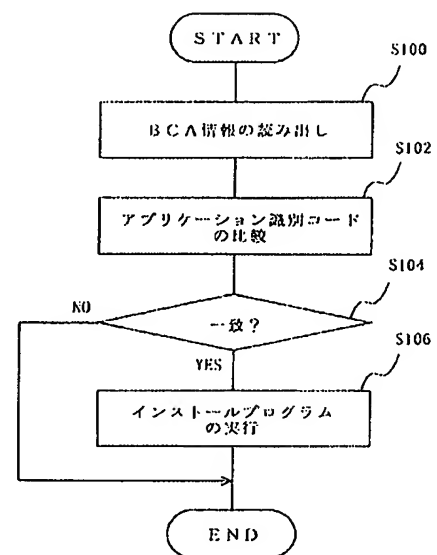
【図1】



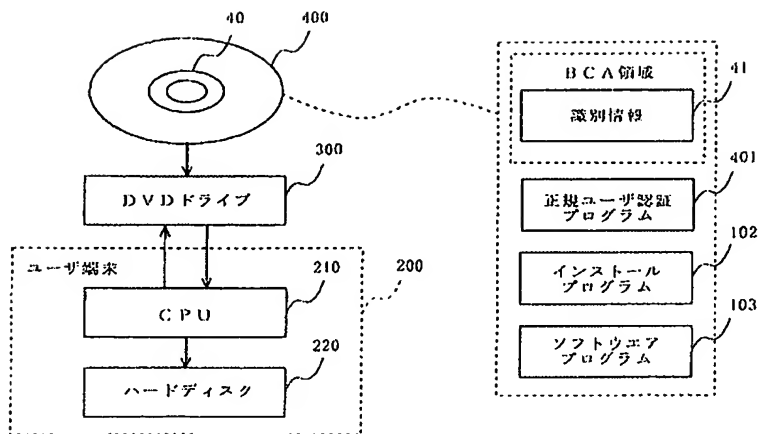
【図2】



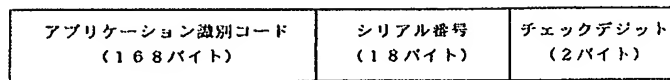
【図3】



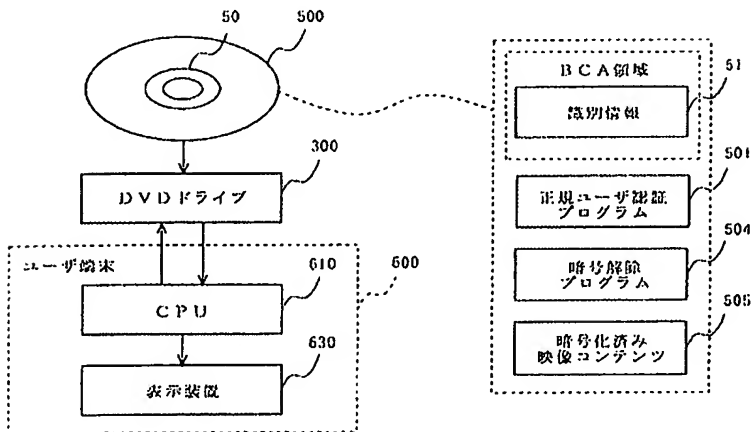
【図4】



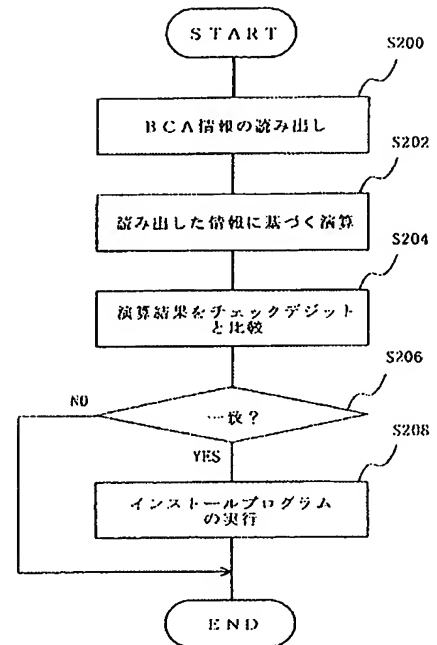
【図5】



【図7】



【図6】



【図8】

